Personnel Safety System Generation-3 Review April 26, 2004

Afternoon Session

Presented by

K. Belcher, A. Boron, J. Carwardine, R. Emerson, M. Fagan, N. Friedman, G. Markovich, V. Nguyen, J. Servino

Argonne National Laboratory

Office of Science
U.S. Department of Energy

A U.S. Department of Energy
Office of Science Laboratory
Operated by The University of Chicago

Tour - 4-ID

Tour Guide

Nick Friedman

PSS Generation-3 Software Design

Software Configuration Management

Roy Emerson

PSS Generation-3 Software Design

- **Software Configuration Management Ground Rules.**
- **Overall Block Diagram of Software Design Process.**
- **Safety and How We achieve it.**
- **Safety Philosophy**
  - Diversity
  - Redundancy
  - Rules

PSS Generation-3 Software Design

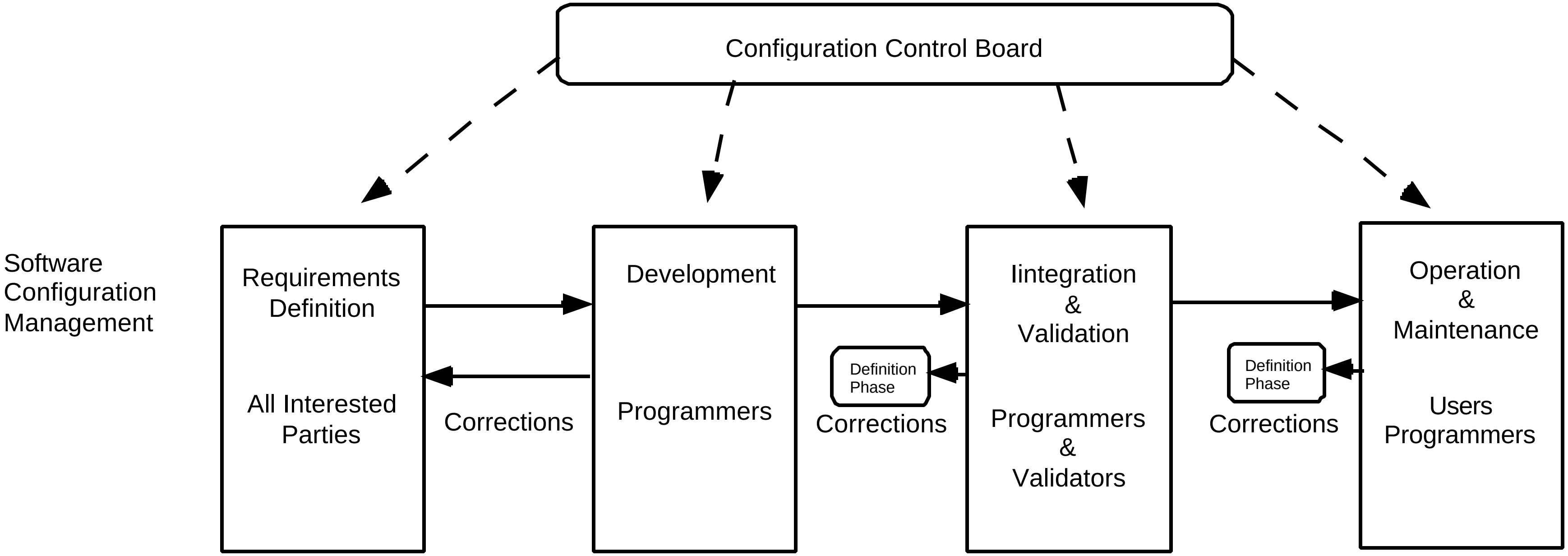
- **Software Configuration Management Plan**
  - Software provides the majority of the safety system functionality.
  - Only part of the total process will be presented here.
  - The SI Group has a documented plan that is used to insure all safety software meets a minimum set of standards.
  - The Plan Goals are:
    - *Assure that controlled and stable baselines are established for planning, managing, and building software systems.*
    - *Assure that the integrity of the system's configuration is controlled over time.*
    - *Assure that the status and content of the software baselines are known.*
  - Software Configuration Management begins with requirements definition and continues for the life of the software.

PSS Generation-3 Software Design

- **The Software lifecycle process**
  - The Configuration Control Board identified in the Configuration Management Overview slide has membership that is both external and internal to the SI Group.
  - The chair for the committee is the PSS System manager.
  - The members of the CCB are:
    - *The SI Group leader.*
    - *The SI Deputy Group leader.*
    - *The programmers for each program chain. (3)*
    - *A floor coordinator representative. (Ray Monroe)*
    - *The beamline coordinator. Varies with each beamline.*
  - The purpose of the CCB is insure everyone involved in defining, developing, deploying and using any given software build has input into the process.

PSS Generation-3 Software Design

Configuration Management Overview



The Software lifecycle

A traditional waterfall approach

PSS Generation-3 Software Design

- **Configuration Management Traceability and Version Control**
  - Traceability to the reviewed baseline software is maintained by an iterative process outlined on the Baseline Traceability slide.
  - As an inherent part of maintaining traceability we simultaneously apply a versioning process to uniquely identify each build of the software.
  - The software and the documents used to build it all carry the same version number and document date to uniquely identify the build set.
  - The complete document set requires review by relevant SI staff and approval by the PSS System Manager.
  - Changes to the baseline requirements affecting any critical device require review and approval by the Beamline Safety Review Committee prior to implementation.

PSS Generation-3 Software Design

- The following set of documents are used to create a specific build of the software and validate it.
  - *System Requirements*
    - Defines core requirements for every system.
  - *Functional Description*
    - Defines functional behavior needed in every system.

PSS Generation-3 Software Design

- *User Requirements (for the specific beamline)*
  - Defines the unique configuration for the beamline.
  - Defines the protective logic used for each shutters critical section.
  - Contains the history of code development for the beamline from initial creation using baseline code and identifying each subsequent modification
    - Modifications are usually required due to beamline configuration changes, but may also be needed to correct code errors.
    - Production code for initial software creation at a beamline will come from either a lab tested software. build or from validated code from another beamline with a similar configuration, never from scratch.

PSS Generation-3 Software Design

  - Production code for builds after the initial software creation will always use the previously validated version for required modifications.
- Number of shutters and the critical section they protect.
- Number of stations
  - Number of doors on each station.
  - Number of search boxes and search path for each station.
  - Number of crash buttons and location in each station.
- Any special issues requiring non standard handling.

PSS Generation-3 Software Design

- *Programmed Fault List (for each programmed chain)*
  - Derived from the system master fault list.
  - Defines the specific faults the system will be programmed to detect (configuration specific).
  - Examples:
    - Remote I/O communication failure (specific to the rack).
    - Door closed failure (specific to the station and door).

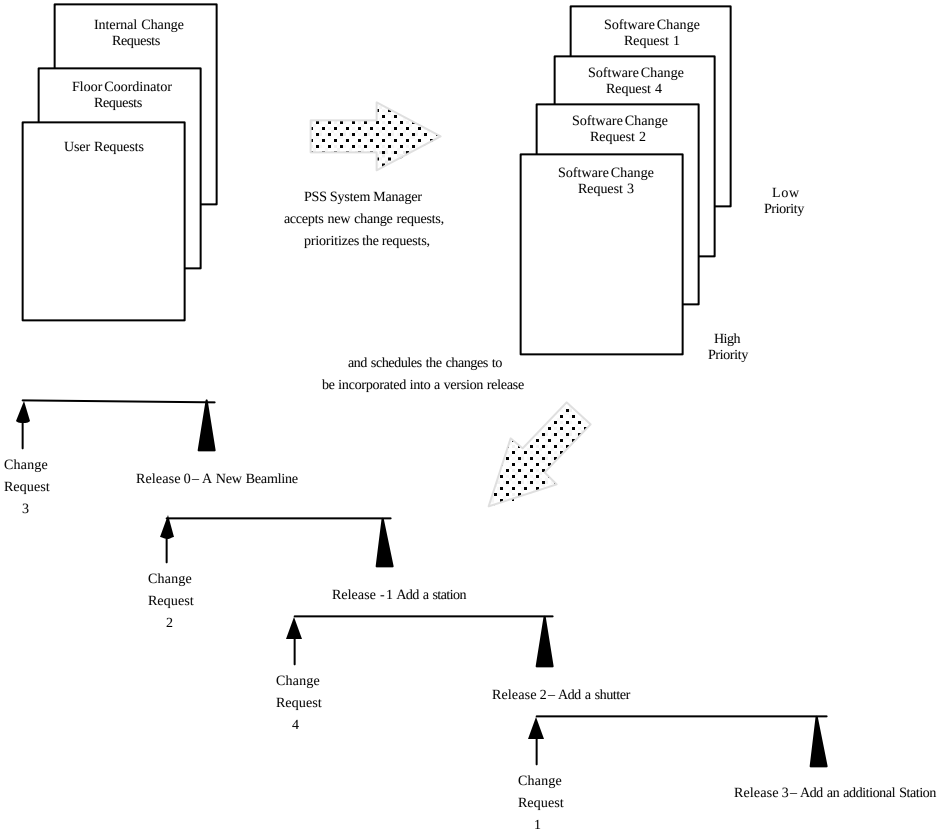
- *Beamline I/O Lists (for each programmed chain)*
  - Derived from the system master I/O list.
  - Defines the I/O mapping to the specific devices at the beamline.

PSS Generation-3 Software Design

- *Software Change Request (SCR)*
  - Details each change to the code item by item.
  - A SCR form is used for each change.
  - Each change is noted by the programmer responsible for the code.
- *Beamline I/O Validation document (for each programmed chain)*
  - Derived from the “Beamline I/O Lists” and used to verify each sensor is wired to the correct input and is operational.
- *Beamline Functional validation (for the specific beamline)*
  - Derived from the System Requirements, Functional Description, User Requirements, Fault List and I/O List.

PSS Generation-3 Software Design

Software Change Request (SCR) Process



Internal Change Requests
Floor Coordinator Requests
User Requests
Software Change Request 1
Software Change Request 4
Software Change Request 2
Software Change Request 3
Low Priority
High Priority
Change Request 3
Release 0– A New Beamline
Change Request 2
Release -1 Add a station
Change Request 4
Release 2– Add a shutter
Change Request 1
Release 3– Add an additional Station

PSS System Manager accepts new change requests, prioritizes the requests,

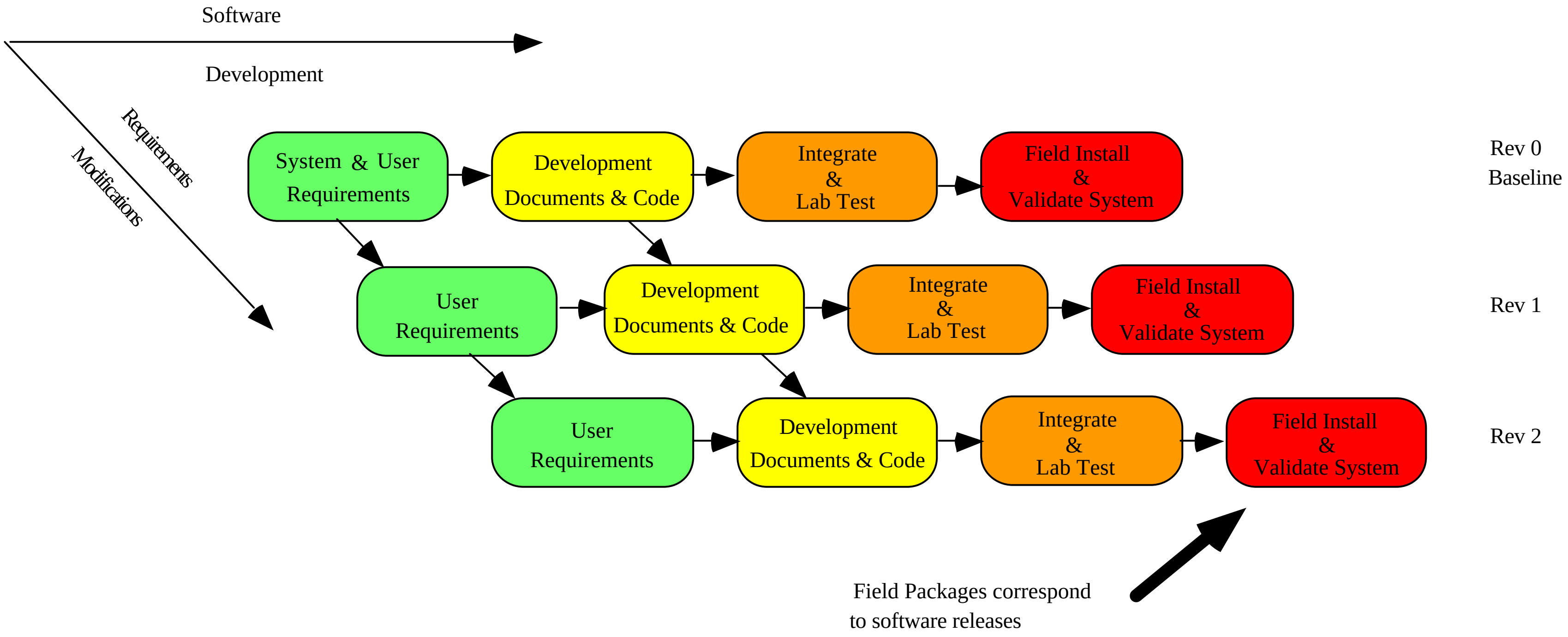
and schedules the changes to be incorporated into a version release

PSS Generation-3 Software Design

- **System wide version control**
  - The software version number and unique beamline ID is encoded by the beamline hardware and in each program to prevent operation of software designed for another beamline or a different version.
- **Baseline Traceability**
  - Version control allows traceability of a specific software build to the specific document set generated for that build for a specific beamline.
  - All software and documents for the most recent 3 validated software builds is archived as an auditable resource.
  - All issues relative to the PSS at all beamlines must be reviewed by or approved by the PSS System manager.

PSS Generation-3 Software Design

Versions required by changes or corrections


Software
Development
Requirements
Modifications
System & User Requirements
Development Documents & Code
Integrate & Lab Test
Field Install & Validate System
Rev 0
Baseline
User Requirements
Development Documents & Code
Integrate & Lab Test
Field Install & Validate System
Rev 1
User Requirements
Development Documents & Code
Integrate & Lab Test
Field Install & Validate System
Rev 2
Field Packages correspond
to software releases

Baseline Traceability

PSS Generation-3 Software Design

- **Archiving and Auditing**
  - The validated code and the associated document set becomes our current set of masters fully identifying the current system configuration.
  - We maintain the last three complete sets of documents and code for backup and audit purposes.
  - The paper copies of the signed documents are filed and are readily accessible through the group secretary.
  - The code and electronic document copies are kept electronically on a server maintained and backed up by APS Information Services.
  - In addition we archive the code and electronic document copies on a CD-R which is stored in a fire proof safe in a separate building.

PSS Generation-3 Software Design

QUESTIONS?

PSS Generation-3 Software Design

- **The next 3 presentations will be about the PSS software.**
- **Each presentation will cover a specific part of the whole system.**
- **Questions that arise may be answered by the time the 3rd presentation is complete.**
- **The system will be presented in the order of:**
  - Chain-A Emergency Shut Down (ESD).
  - Chain-B Emergency Shut Down (ESD).
  - Chain-C Command and Control
    - *Provides the user interface and EPICS interface to the world.*

PSS Generation-3 Software Design Chain-A

Anne Boron

PSS Generation-3 Software Design Chain-A

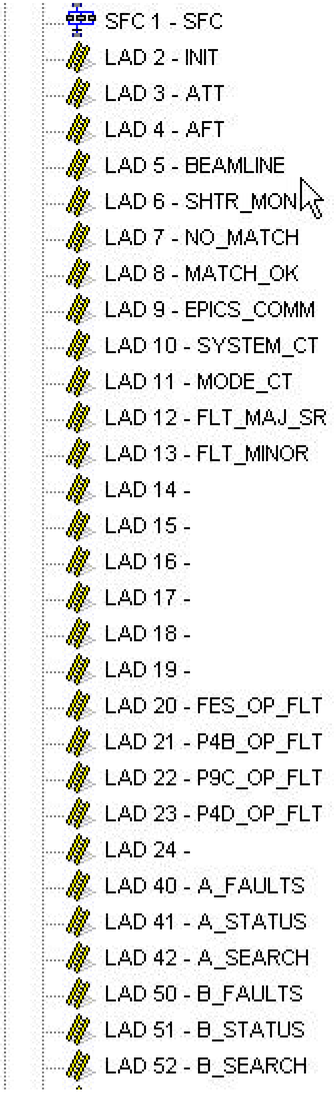
- **Overview:**
  - Chain A is first of three chains in PSS Gen 3.
  - Chain A contains primarily ESD code.
  - Several “Level One” items/major faults are contained in Chain A code.
  - What is the path of a minor fault through the system?

PSS Generation-3 Software Design Chain-A

- **Chain-A is the first of three chains in PSS Gen. 3**
  - Composed of Allen Bradley Control Logix Hardware
    - *Main PLC rack (with CPU) is on Mezzanine level.*
    - *Remote I/O racks are located at beamline stations.*
    - *Communication between Mezzanine rack and Remote racks done via Control Net.*
  - Communicates to Chain C via Profibus.
  - Ethernet module used strictly for code downloads.

PSS Generation-3 Software Design Chain-A

- **Chain-A Code**
  - Contains primarily ESD functions
    - *Exception: Search sequences remain in Chain A.*
  - Files structured to separate beamline functions and station functions, diagnostics, and data collection.



SFC 1 - SFC
LAD 2 - INIT
LAD 3 - ATT
LAD 4 - AFT
LAD 5 - BEAMLINE
LAD 6 - SHTR_MON
LAD 7 - NO_MATCH
LAD 8 - MATCH_OK
LAD 9 - EPICS_COMM
LAD 10 - SYSTEM_CT
LAD 11 - MODE_CT
LAD 12 - FLT_MAJ_SR
LAD 13 - FLT_MINOR
LAD 14 -
LAD 15 -
LAD 16 -
LAD 17 -
LAD 18 -
LAD 19 -
LAD 20 - FES_OP_FLT
LAD 21 - P4B_OP_FLT
LAD 22 - P9C_OP_FLT
LAD 23 - P4D_OP_FLT
LAD 24 -
LAD 40 - A_FAULTS
LAD 41 - A_STATUS
LAD 42 - A_SEARCH
LAD 50 - B_FAULTS
LAD 51 - B_STATUS
LAD 52 - B_SEARCH

PSS Generation-3 Software Design Chain-A

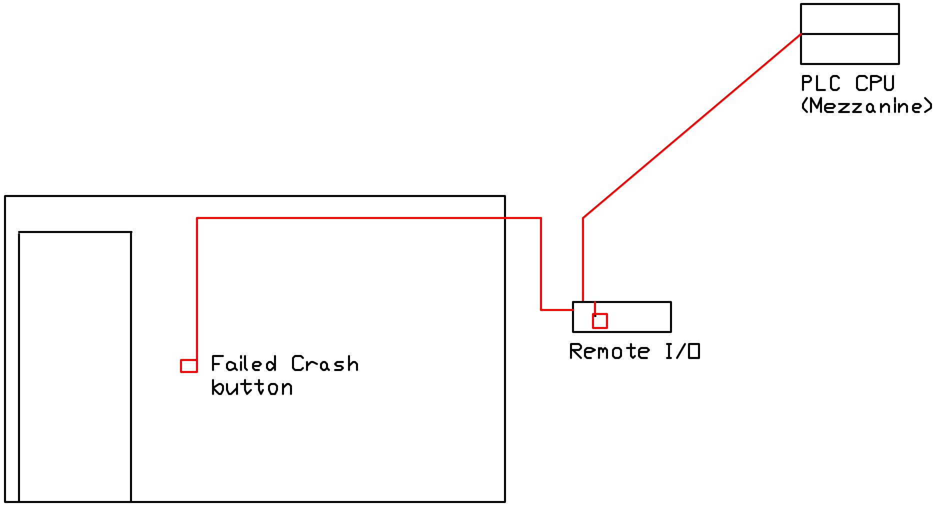
- **“Level One” items: What will cause Chain A to pull shutter and storage ring permits?**
  - “Level One” items are classified as major faults in the PLC software program.
  - “Level One” items/Major faults include:
    - *Crash button depressed or failed when the station is beam active.*
    - *Door opened or door switch failed when the station is beam active.*
    - *When any unsearched station becomes beam active.*

PSS Generation-3 Software Design Chain-A

- **Minor Faults:**
  - Purpose of minor fault is to warn beamline users of a failure in the system and to inhibit beam until said failure is remedied. Minor faults will NOT dump the storage ring.
  - What are Minor faults?
    - *Minor faults include signal losses and switch failures that do not immediately create a life threatening situation. Minor faults include PLC watchdog faults, Test box open faults, loss of Global Online, PLC key in Remote position, Forces present in PLC, 24VDC power failure, shutter switch faults (not beam active), pressure and flow faults, communications faults, and crash button faults (not beam active).*

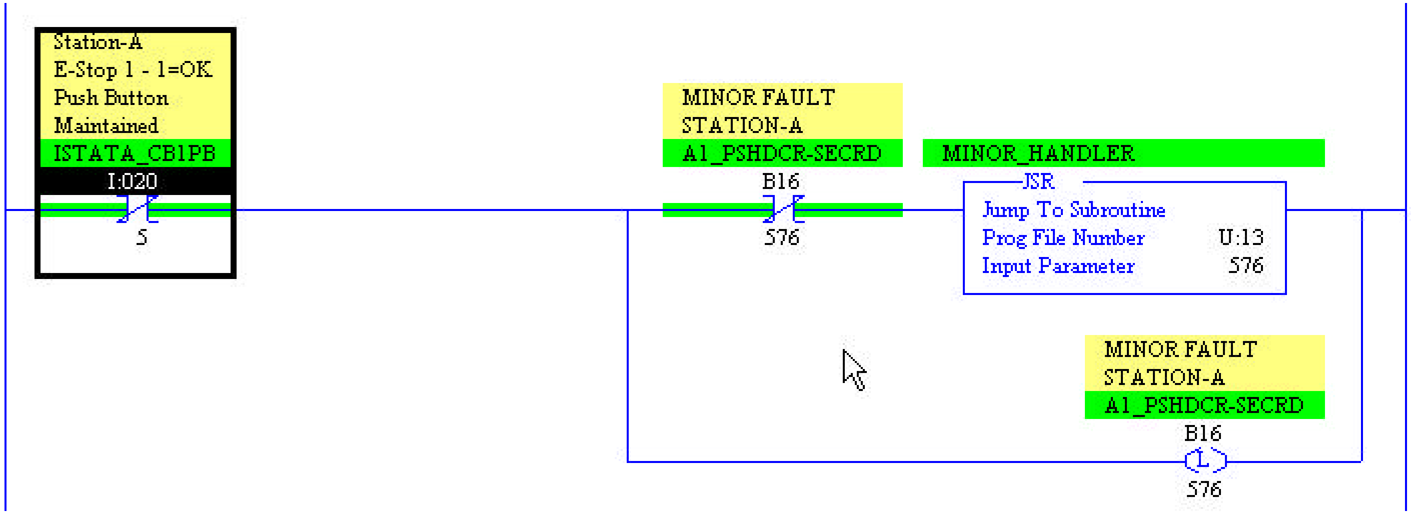
PSS Generation-3 Software Design Chain-A

- **What happens when a minor fault occurs?**
  - Hardware fails.
  - Change of signal from failed hardware in I/O block.
  - Signal from I/O block processed in PLC logic.



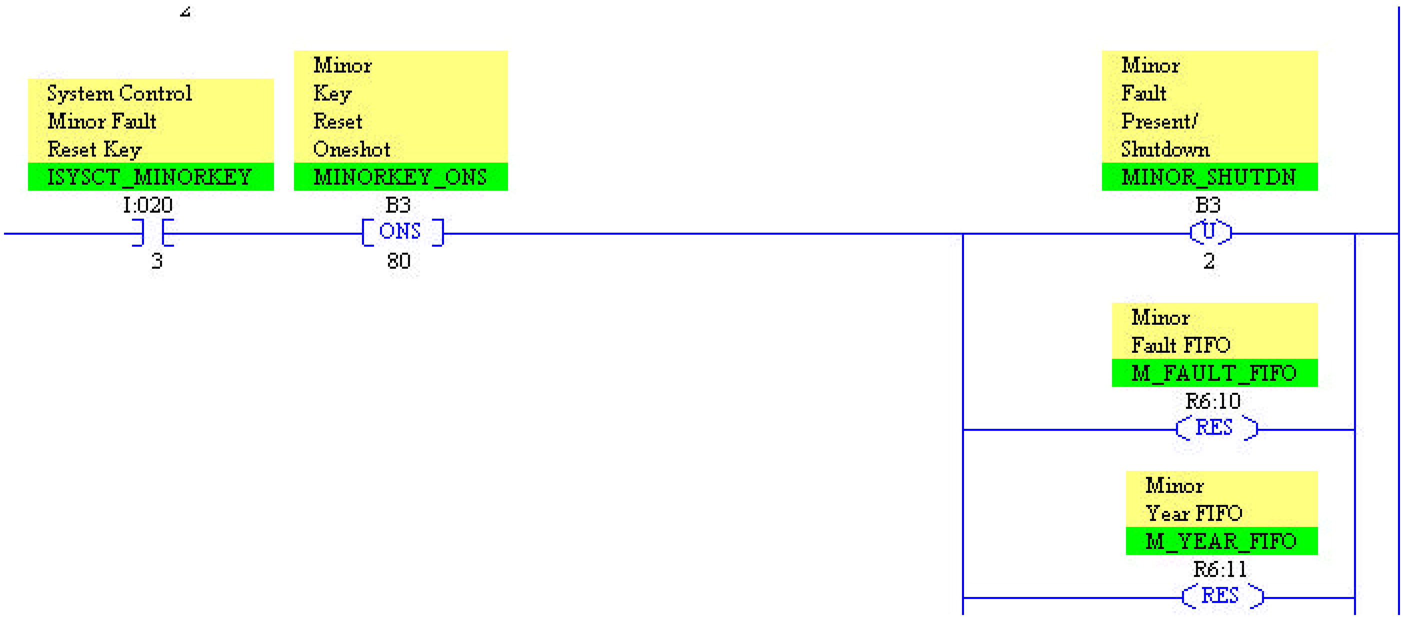
PSS Generation-3 Software Design Chain-A

- **What happens when a minor fault occurs? (continued)**
  - Fault logic rung solves true.
  - Fault subroutine called, fault reported to Chain C.
  - Fault situation latches bits “on.”



PSS Generation-3 Software Design Chain-A

- **What happens when a minor fault occurs? (continued)**
  - Shutter permit(s) removed.
  - All shutters close.
  - System remains latched in faulted state until fault situation remedied and fault is reset by key action.



PSS Generation-3 Software Design Chain-A

- **Summary**
  - Chain A is first of three chains in PSS Gen 3, and contains primarily ESD code as well as search and secure routines.
  - "Level One"/major fault items in the code include crash button faults and door switch loss when beam active, and when beam is introduced into unsearched stations.
  - Minor faults include crash button failures in searched stations, pressure faults, communications faults, flow faults and most shutter faults.

PSS Generation-3 Software Design Chain-A

Questions?

On To Chain B….

PSS Generation-3 Software Design Chain-B

PSS Chain-B

General Structure + Specific example of how an emergency shut down is handled all the way to the HMI

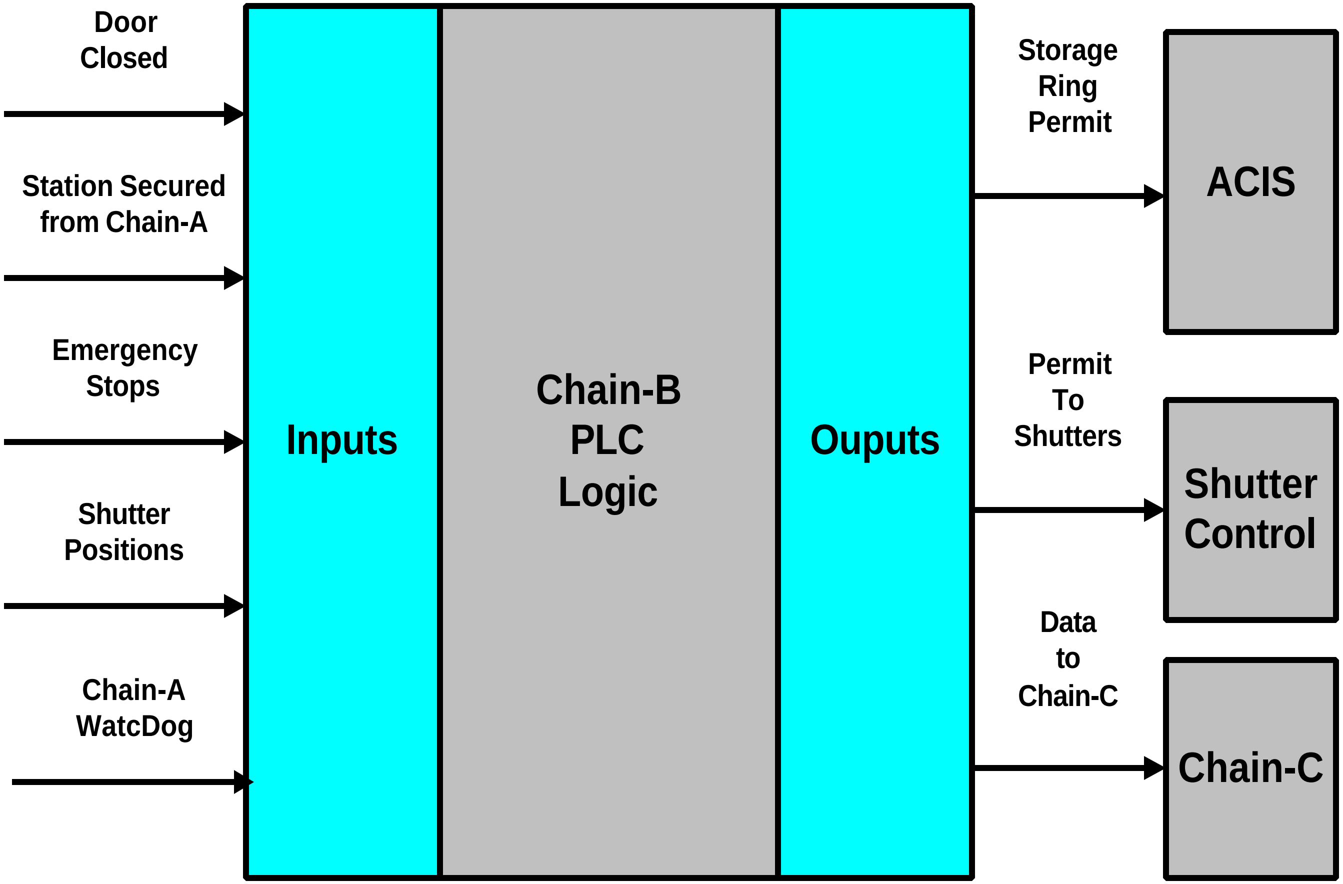
Van Nguyen

PSS Generation-3 Software Design Chain-B

- **System Overview**
- **Functions**
- **Fault Detection - Major Fault Example**
- **Data to Chain-C**

PSS Generation-3 Software Design Chain-B

- **System Overview - Emergency Shut Down (ESD).**



PSS Generation-3 Software Design Chain-B

- **Emergency Shut Down (ESD)**
  - A shutdown will occur, if the there is a potential of exposure to prompt radiation.

- **Functions**
  - Enables Permits
    - *Storage Ring.*
    - *Front End Shutters.*
    - *Integral Shutter / Mode Shutters.*
  - Monitors Critical Components For Issuing Permits
    - *Doors Switch.*
    - *Emergency Stop.*
    - *Manual Beam Stops.*

PSS Generation-3 Software Design Chain-B

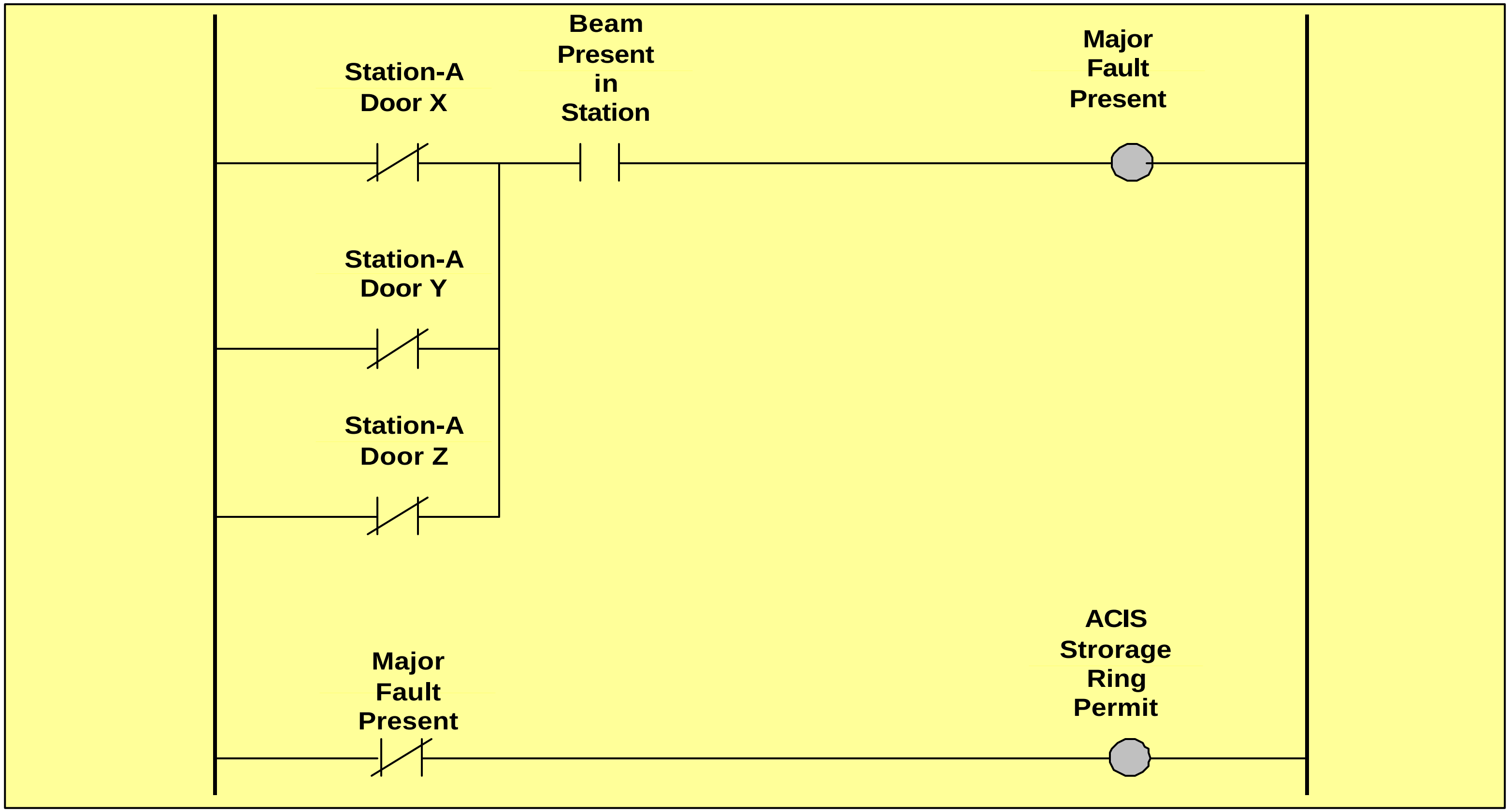
- **Fault Detection**
  - ESD Chain-B also has two categories of faults Major or Minor.

- **ACIS Storage Ring Permit**
  - Any Major Faults will turn off the “ACIS Storage Ring Permit”
  - this is an immediate loss of stored beam.

- **Conditions for Major Faults**
  - When beam is present in a station and any door closed switch is OFF, in that station (assumed beam is present when shutter closed switch is OFF).
  - When beam is present in a station and any Crash Button (Emergency Stop) is pressed, in that station.
  - When beam is present in a station and that station is not search & secured.

PSS Generation-3 Software Design Chain-B

- **Example logic of a Major Fault**
  - Beam is present in a station and any door closed switch is OFF, in that station.



PSS Generation-3 Software Design Chain-B

- **Data to Chain-C**
  - Transmit data to Chain-C
    - *Inputs- Door position switches / Shutter position.*
    - *Outputs-Permits.*
    - *Misc. Data.*
  - Major & Minor Faults
    - *Send detail message of each failure.*
    - *These messages will aid troubleshooting.*

QUESTIONS?

PSS Generation-3 Software Design

PSS Chain-C – General Structure – HMI and EPICS

(Specific example of how an ESD is handled all the way to the HMI & EPICS)

John Servino

PSS Generation-3 Software Design Chain-C

- **Chain-C Command & Control System**
  - System Architecture Overview.
  - Application Specific Communications – Database.
  - EPICS & HMI.
  - Software Architecture.

PSS Generation-3 Software Design Chain-C

- **Application Specific Communication**

  - Master Database - Reside In Chain-C
    - All Signals: Chain-A, Chain-B, Chain-C, EPICS & HMI.

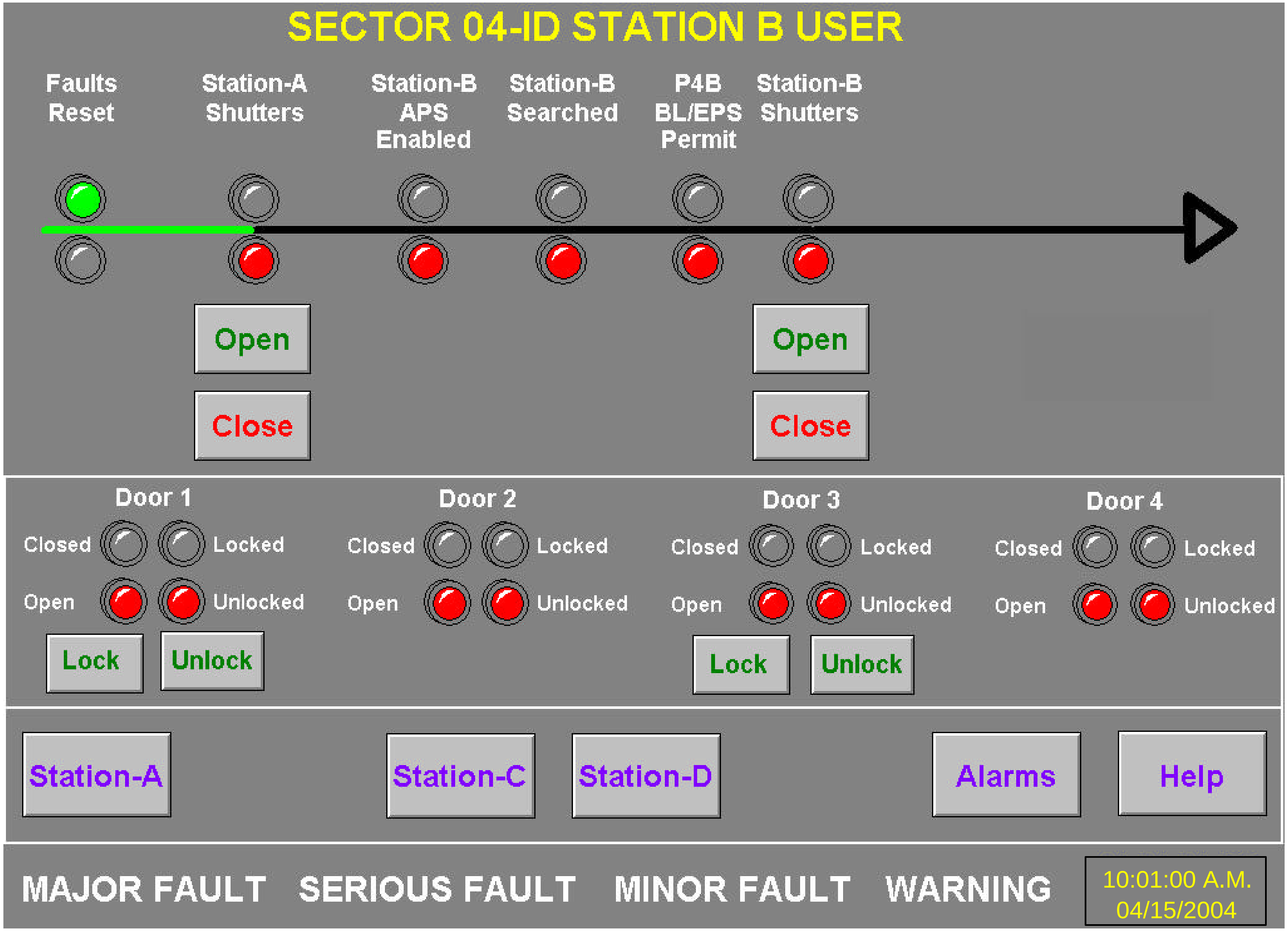
  - Chain-A & Chain-B
    - One-way Communications From Chain-A To Chain-C.
    - One-way Communications From Chain-B To Chain-C.
    - All Inputs & Outputs ,Faults & Specific Status Signals.

  - EPICS & HMI
    - Bi-directional Communications To Chain-C.

PSS Generation-3 Software Design Chain-C

- **HMI & EPICS**
  - PSS HMI - Panelview Plus Touch Screen.
  - EPICS - Computer Platform Database & HMI.
  - Access To All Signals In The Chain-C Database.
  - Display Status, Faults & Diagnostics
    - Indicator / Animated Bitmap.
  - Control Shutter Operation.

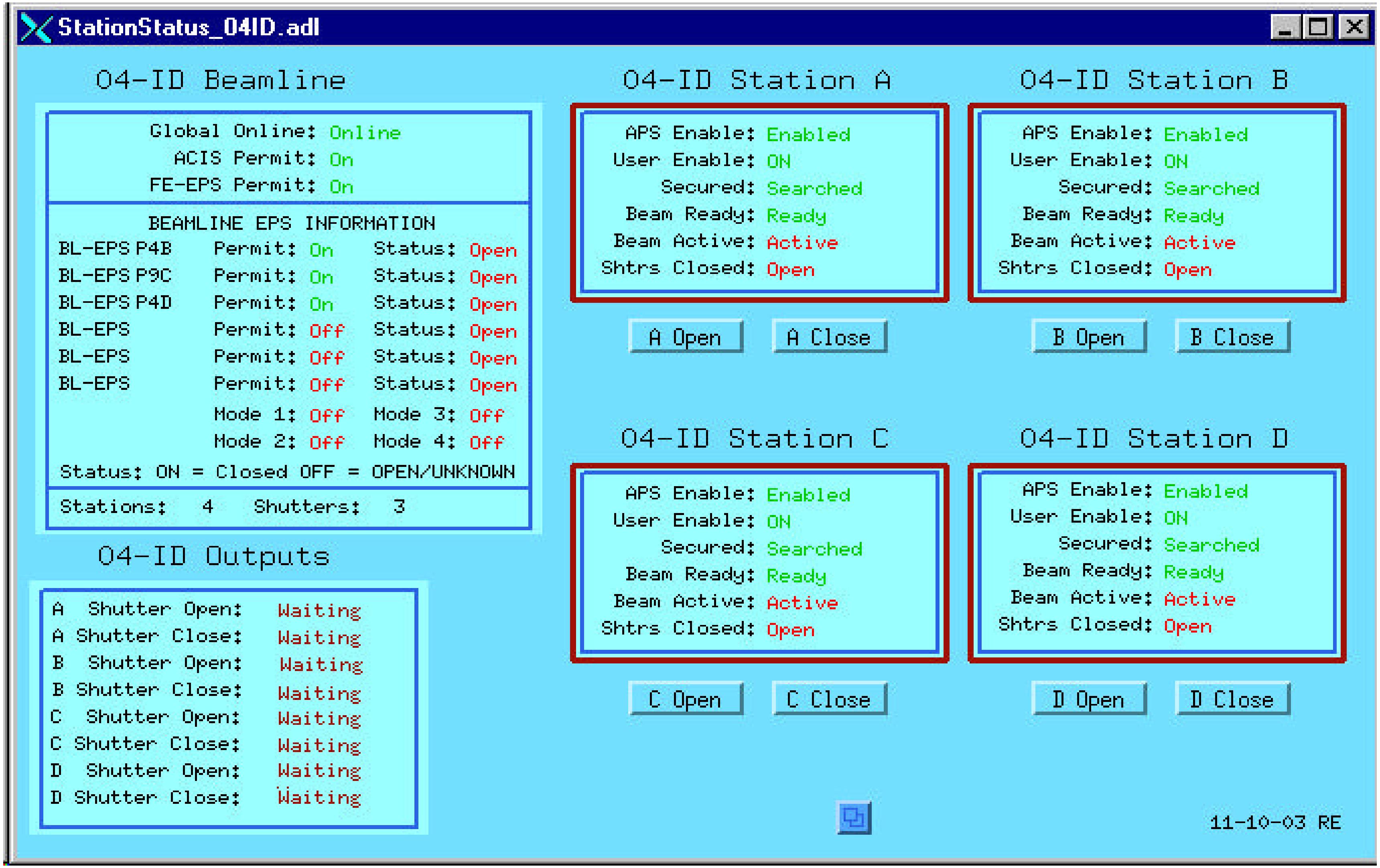
PSS Generation-3 Software Design Chain-C



SECTOR 04-ID STATION B USER

10:01:00 A.M.
04/15/2004

PSS Generation-3 Software Design Chain-C



StationStatus_04ID.adl

```
04-ID Beamline

        Global Online: Online
          ACIS Permit: On
       FE-EPS Permit: On

       BEAMLINE EPS INFORMATION
BL-EPS P4B   Permit: On    Status: Open
BL-EPS P9C   Permit: On    Status: Open
BL-EPS P4D   Permit: On    Status: Open
BL-EPS       Permit: Off   Status: Open
BL-EPS       Permit: Off   Status: Open
BL-EPS       Permit: Off   Status: Open
             Mode 1: Off   Mode 3: Off
             Mode 2: Off   Mode 4: Off
Status: ON = Closed OFF = OPEN/UNKNOWN
Stations:  4   Shutters:  3
```

```
04-ID Outputs

A  Shutter Open:   Waiting
A Shutter Close:   Waiting
B  Shutter Open:   Waiting
B Shutter Close:   Waiting
C  Shutter Open:   Waiting
C Shutter Close:   Waiting
D  Shutter Open:   Waiting
D Shutter Close:   Waiting
```

```
04-ID Station A

  APS Enable: Enabled
 User Enable: ON
     Secured: Searched
  Beam Ready: Ready
 Beam Active: Active
Shtrs Closed: Open
```

```
04-ID Station B

  APS Enable: Enabled
 User Enable: ON
     Secured: Searched
  Beam Ready: Ready
 Beam Active: Active
Shtrs Closed: Open
```

```
04-ID Station C

  APS Enable: Enabled
 User Enable: ON
     Secured: Searched
  Beam Ready: Ready
 Beam Active: Active
Shtrs Closed: Open
```

```
04-ID Station D

  APS Enable: Enabled
 User Enable: ON
     Secured: Searched
  Beam Ready: Ready
 Beam Active: Active
Shtrs Closed: Open
```

11-10-03 RE

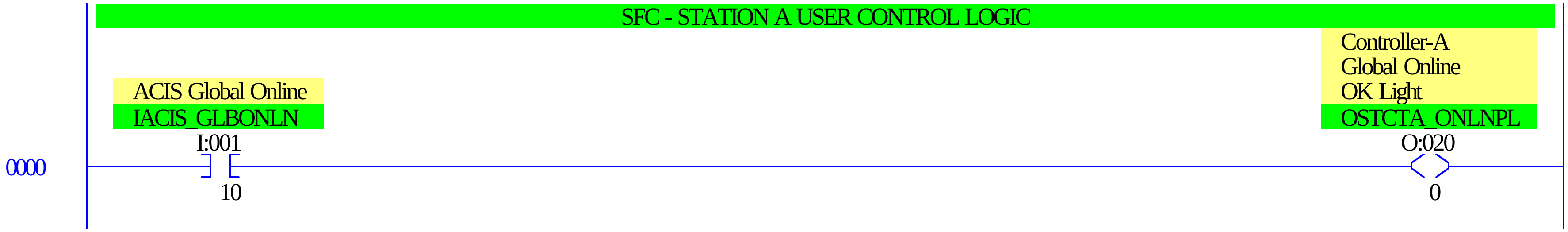
PSS Generation-3 Software Design Chain-C

- **Software Architecture**
  - Programming Environment.
  - Command & Control Functions.
  - Chain-A & Chain-B Signal Processing.
  - Fault Detection & Diagnostics.

PSS Generation-3 Software Design Chain-C

PLC Programming Environment

- Allen Bradley / Rockwell Software.
- RSLogix5000 & RSNetworks For ControlNet.
- Ladder Logic & Structured Text Programming.
- Hardware Configuration: Local & Remote-I/O / Profibus / Etc.



```
(* CONVERT THE TIME AND DATE TO A USER DEFINED INTEGER DATA FORMAT    *)

CURRENT_TIME := NOW;
CURRENT_SEC_MIDNIGHT :=  TIME_TO_REAL(CURRENT_TIME-MIDNIGHT);
ACTUAL_TIME_DATE.TIME_DATE[5] :=   CURRENT_SEC_MIDNIGHT MOD 60;
ACTUAL_TIME_DATE.TIME_DATE[4] :=  (CURRENT_SEC_MIDNIGHT MOD 3600)/60;
ACTUAL_TIME_DATE.TIME_DATE[3] :=   CURRENT_SEC_MIDNIGHT / 3600;
```

PSS Generation-3 Software Design Chain-C

- **Primary Command & Control Functions**

  - Shutter Control
    - Front End - Sequenced Shutter.
    - Integral - Sequenced / Non-sequenced Shutters.
    - Mode Shutter Control & Configuration.

  - Door Control
    - Pneumatic Doors.
    - Manual Doors.

PSS Generation-3 Software Design Chain-C

- **Shutter Control**
  - Front End Shutter (FES)
    - Chain-A Sends “FES Open Permit” Via Comm Link.
    - Chain-B Sends “FES Open Permit” Via Comm Link.
    - Chain-C Checks All FES Open Permits Via Inputs.
    - No Chain-A / B / C Faults.

    - The FES Will Be Sequenced Open When:
      - The HMI or EPICS Issues A FES Open Request.

    - The FES Will Be Sequenced Closed When:
      - The HMI or EPICS Issues A FES Close Request.
      - Any FES Permit Transitions Off - Station User Key.
      - Any Chain-A / B / C Fault.

PSS Generation-3 Software Design Chain-C

- **Shutter Control Continued**
  - Integral Shutters
    - Chain-A Sends “Shutter Open Permit” Via Comm Link.
    - Chain-B Sends “Shutter Open Permit” Via Comm Link.
    - Chain-C Checks All Shutter Open Permits Via Inputs.
    - No Chain-A / B / C Faults.

    - They Will Be Open When (Sequenced If Required):
      - The HMI or EPICS Issues A FES Open Request.

    - They Will Be Closed When:
      - The HMI or EPICS Issues A FES Close Request.
      - Any Shutter Permit Transitions Off - BLEPS Permit.
      - Any Chain-A / B / C Fault.

PSS Generation-3 Software Design Chain-C

- **Door Operation**

  - Pneumatic Doors
    - Unlock & Open Control.
    - Close & Lock Control.
    - Door Status To HMI And Door Control Panel.
    - Beep/Buzz Logic For Door Control Panel.

  - Manual Doors
    - Unlock & Lock Control.
    - Door Status To HMI.

PSS Generation-3 Software Design Chain-C

- **Additional Command & Control Functions**
  - Process Chain-A / B / C Info For HMI & EPICS.
  - Process Hardwired Signals To Chain-A & B.
  - Beep/Buzz Logic For Station User Panels.

PSS Generation-3 Software Design Chain-C

- **PSS Application Fault Detection-Derived From PLC Inputs**
  - Chain-C Generates Only Minor Faults & Warnings
    - Minor Fault - Door Close Switch Failure.
    - Minor Fault - Crash Button Pressed.
    - Warning - Door Lock Switch Failure.
  - Chain-A & B Major & Minor Faults
    - Integrated Into Logic.
    - Used To Bypass Specific Minor Faults (Crash Button).

PSS Generation-3 Software Design Chain-C

- **Control Logic PLC Fault Detection-Derived By Allen Bradley**

  - Minor Faults
    - PLC Force Present.
    - Remote I/O Communication Loss.

  - Warning
    - PLC Battery Low.

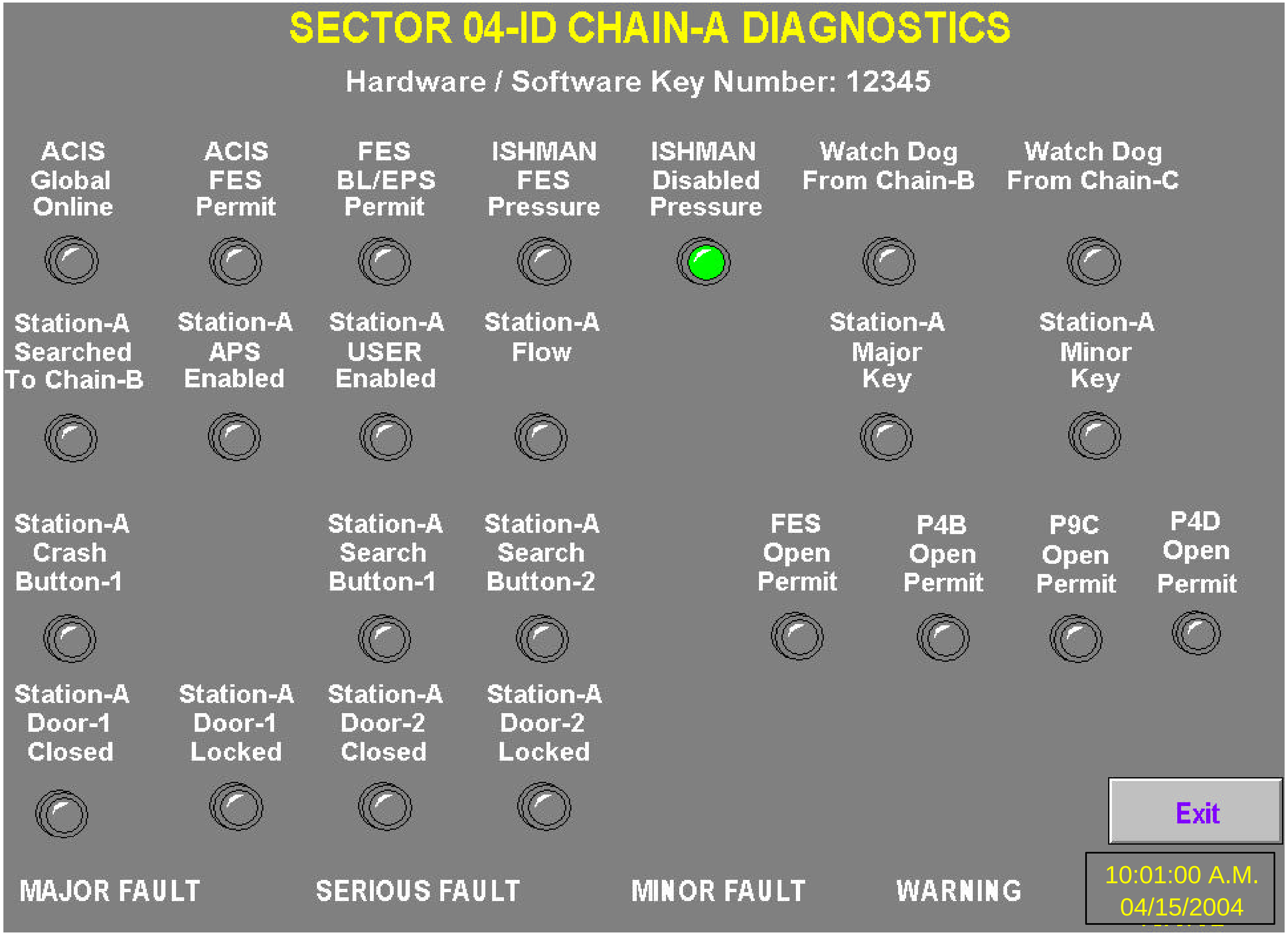
PSS Generation-3 Software Design Chain-C

- **End To End Example**
  - Follow the Path Of A Major Fault In Chain-A Through The HMI
    - Crash Button Pressed While The Station Is Beam Active.

PSS Generation-3 Software Design Chain-C

- **Diagnostics**
  - Displayed On The HMI & EPICS Screens
    - Indicator Red/Green.
    - Animated Bitmap Drawing.

PSS Generation-3 Software Design Chain-C



SECTOR 04-ID CHAIN-A DIAGNOSTICS

Hardware / Software Key Number: 12345

10:01:00 A.M.
04/15/2004

PSS Generation-3 Software Design Chain-C

QUESTIONS?

Validation System Cart

Van Nguyen

Validation System

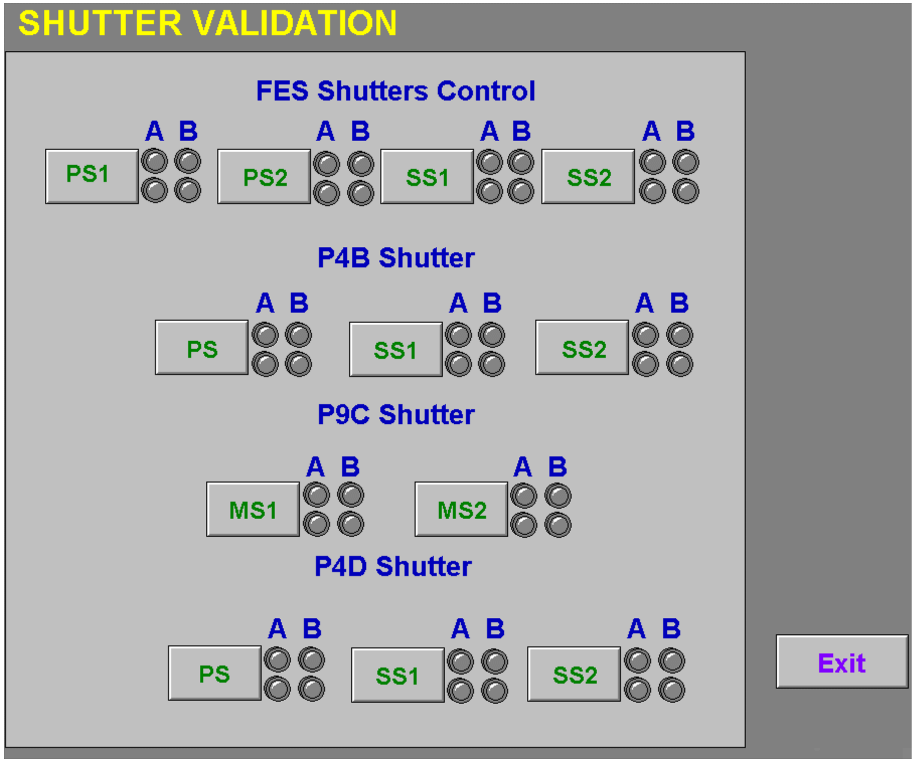
- Functions
- Features
- Validation Process

Validation System Functions

- **Emulate Critical ESD Field Devices**
  - Point to point techniques is used to inject signal.
  - Logic may or may not be necessary to emulate device behaviors.
  - **Front End Shutters**-logic is necessary to emulate cylinder closing in sequence and timing delays.
  - **Doors**-logic is necessary to emulate lock and magnetic bond sensors.
  - **Crash Button**-point to point injections.
- **Simulate Other Systems**
  - During validations if other systems are not available, therefore their interfaces are simulated.

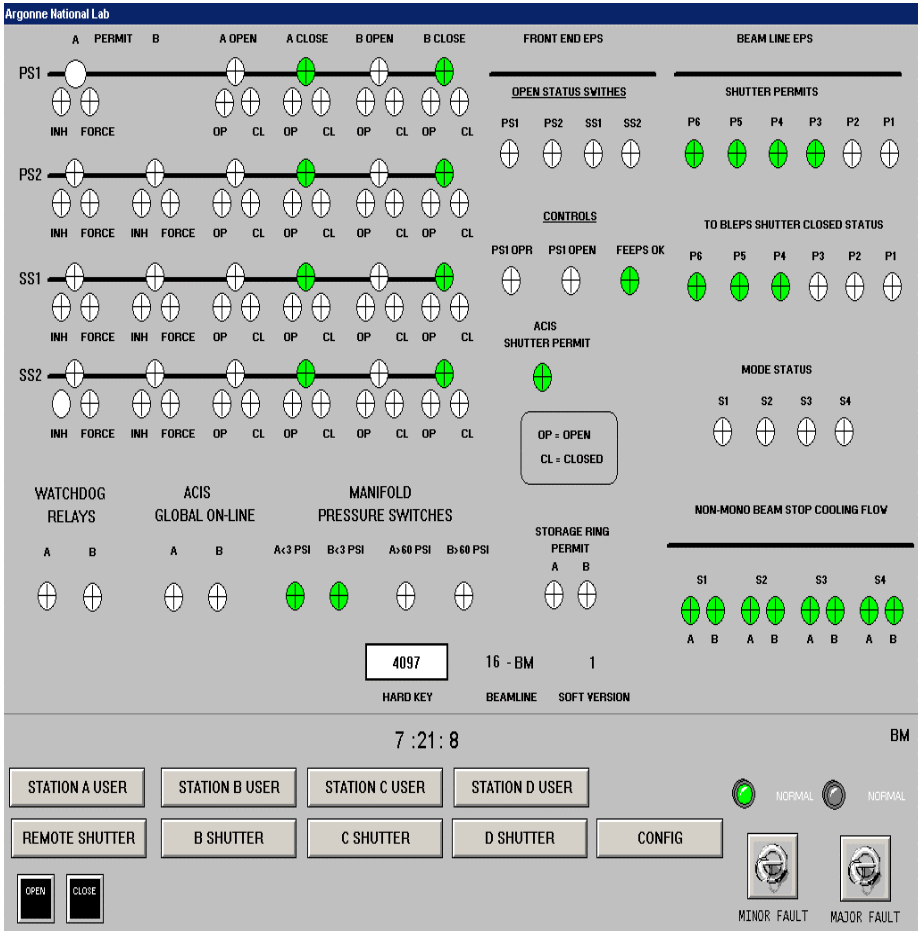
Validation System Functions

- **Interface panel**
  - Each device is represented by a soft pushbutton or soft LED, on the HMI panel.
  - Clicking a pushbutton will inject 24v to the associated I/O address to the ESD system.



Validation System Functions

- **Simulate Interfaces**
  - ACCESS Control Interlock System (ACIS).
  - Front End Equipment Protection System (FEEPS).
  - Beam Line Equipment Protection System (BLEPS).



Validation System Features

- **Generation-1 System**
  - Fault conditions are manually created.
  - Test Setup Conditions are time consuming.
  - Invasive methods-disconnecting field device to connect test equipments.
- **Generation-3 Validation System**
  - Non-invasive.
  - Reduce test steps.
  - Control and interfaces are done at one location.
  - Inject test scenarios with a push of a button.

Validation Process

- **Validations are conducted in three phases**
  - **I/O Check-Out to verify continuity**
    - Actuate each device and observe that the input is validated (PLC image tables).
    - Enable each output and observe that the associated device is active.
  - **Validate beamline using the Validation System**
    - Connect Validation System to beamline and test the ESD code.
  - **Post Validation System**
    - Disconnect Validation System.
    - Transfer the system back to operating mode.
    - Then an end-to-end test is performed.

PSS Generation-3 Validation System

QUESTIONS?

Laboratory Simulator

Anne Boron

“Hardware in the Loop” Beamline Simulator

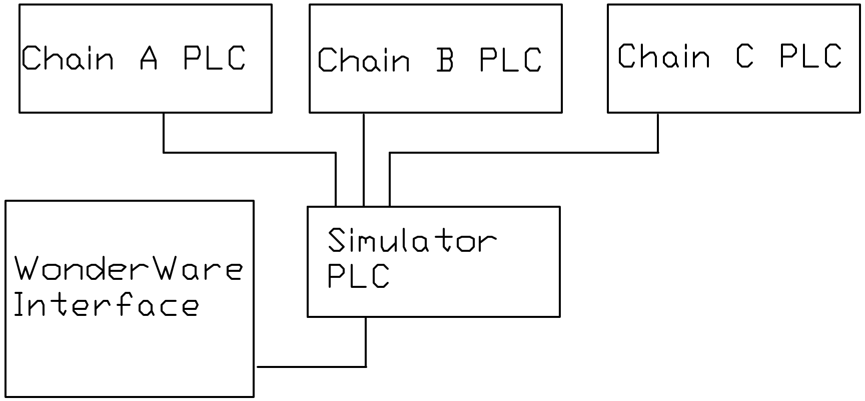
- **Overview**
  - What is the intended purpose of the simulator?
  - What will the elements of the system be?
  - How will it work?
  - What will be the paths for program logic?

“Hardware in the Loop” Beamline Simulator

- **Purpose:**
  - To allow for testing of beamline PSS Code in laboratory both to eliminate time lost in validations performed on the floor and to test “what if” scenarios. All Generation 3 software code will be developed using this system
    - *Virtual Beamline will be created.*
    - *Virtual switches will send inputs to PLCs.*
    - *Virtual shutters will be programmed to open and close.*
    - *Virtual doors will open and close upon request.*

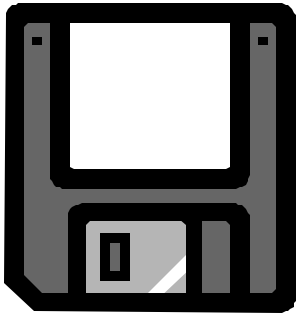
“Hardware in the Loop” Beamline Simulator

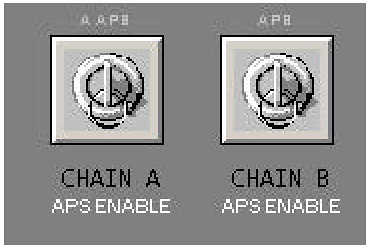
- **What will make up the system?**
  - PLC hardware for Chains A, B, and C.
  - Simulator PLC and program (using Wonderware Intouch interface).
  - System will be modular and can be easily adapted to each beamline’s unique elements.



"Hardware in the Loop" Beamline Simulator

- **How will it work?**
  - Exact code which will be sent to floor will be extensively tested.
  - Exact validation procedure will be followed.
  - Signals on simulated panels will be separated by PLC chain where required (i.e.: Chain A door open switch, Chain B door open switch).



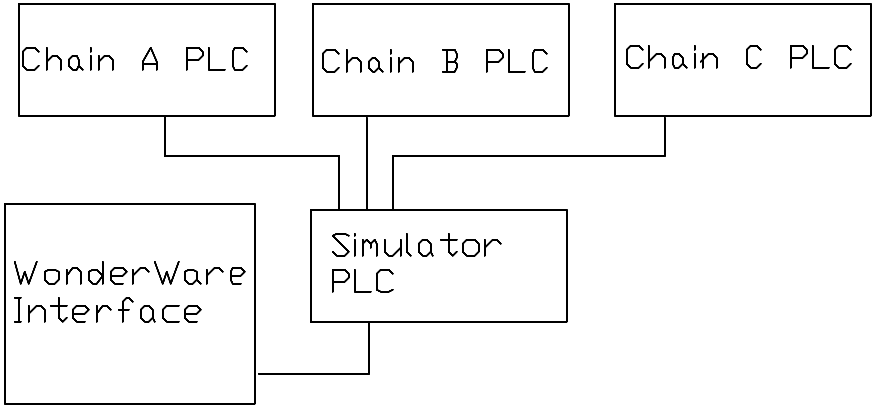


“Hardware in the Loop” Beamline Simulator

- **Program Logic**
  - Some signals will be directly mapped to outputs in the Simulator PLC, such as crash buttons and panel lights
    - *Input will be sent to the system via virtual switch programmed into Wonderware Intouch interface.*
    - *A corresponding bit will be set high.*
    - *The “on” signal will be transmitted directly to Chain A, B, or C as a program input.*
    - *The signal will then travel the reverse path back to the indicator lights and outputs on the simulator panel.*

"Hardware in the Loop" Beamline Simulator

- **Program Logic (Continued)**
  - Some signals will require program action in simulator PLC, such as door or shutter movement (timing)
    - *Input will be sent to system via virtual switch programmed into Wonderware Intouch interface.*
    - *A corresponding bit will be set high.*
    - *Program will run, output will be generated.*



“Hardware in the Loop” Beamline Simulator

- Signals requiring program action continued….
  - *The “on” signal will be transmitted from the simulator PLC as an output to Chain A, B, or C as a program input.*
  - *The signal then will travel the reverse path back to the indicator lights on the simulator panel which show the result of the action.*

“Hardware in the Loop” Beamline Simulator

- **Review**
  - The purpose of the simulator will be to pre-test the software code.
  - The system will contain all three PLC chains as well as an interface to simulate inputs and simulator PLC hardware.
  - The system will simulate beamline hardware and test the exact code using the exact validation procedure before the code goes to the floor.
  - Much simulator logic will be sent as a 1 to 1 signal, but some events, such as door and shutter opening and closing require further program processing (timing).

“Hardware in the Loop” Beamline Simulator

QUESTIONS?

Upgrading Existing Systems

Path for retrofitting key functionality to existing systems.

Roy Emerson

Upgrading Existing Systems

- **Option-1, Retrofit the entire Gen-1 PSS to Gen-3 PSS.**
- **Option-2, Implement Non-invasive Testing into Gen-1 PSS.**
- **Option-3, NO UPGRADE - Purchase surplus of Gen-1 Hardware.**

Upgrading Existing Systems

- **Option-1, Retrofit the entire Generation-1 to Generation-3 PSS**
  - *Replace Chain-A & Chain-B PLC.*
  - *Add Chain-C PLC & HMI.*
  - *Replace FERDP with Mezzanine PCB.*
  - *Re-terminated field wiring on PCB.*
  - *Replace the Generation-1 Station control panel (15U) with a Generation-3 control panel (included Station PCB)*
    - Panel size has same form factor, fit in same location.
  - *Field wiring re-terminated on PCB.*

Upgrading Existing Systems

- **Option-2, Implement Non-invasive Testing into Gen-1 PSS**
  - Replace FERDP with a Gen-1 retrofit Mezzanine PCB
    - *Re-terminate field wiring to PCB.*
  - Modify Station enclosure (15U), which includes Gen-1 retrofit Station PCB
    - *Re-termination field wiring to PCB.*

NOTE: Both Mezzanine and Station systems need to modified to implement Non-Invasive testing feature.

Path for Retrofitting

QUESTIONS?

Statement of Work
Migration from Generation-1 to Generation-3
and
Feature comparison of Generation-1 to Generation-2 and Generation-3

Roy Emerson

Statement of Work – Our Goals

- **Our Goals**
- **Operations and Safety**
  - The PSS system must meet Safety, Reliability and Operational needs of the APS and users.
  - We will first talk about some but not all of the ways we meet the safety requirements of DOE, ES&H, APS and the User community.
  - Second we will discuss how we plan to achieve reliability.
  - Last we will explain the operational aspects of the PSS.

Operational and Safety Considerations

- **Meet the safety and operational needs of the APS beamlines in a cost-effective manner.**
  - Safety Compliance with DOE 5480.25 and 420.2a.
  - 1.F.2.b Technical Design
    - *(1) Fail Safe design*
      - All protective functions are designed for fail-safe operation.
      - Unsafe conditions require energized complete circuits.
    - *(2) No single point failure*
      - All critical devices are duplicated in each chain.
    - *(3) Component protection*
      - All PSS wiring and systems in dedicated racks, cable trays, and armored conduit.

Operational and Safety Considerations

- 1.F.2.b Technical Design - continued
  - *(4).(a) Redundant critical devices*
    - All critical devices have a backup.
  - *(4).(b) Redundant status of critical devices*
    - Both chains independently monitor all critical devices.
  - *(7) Modular Design*
    - Components of the PLC systems are of modular design for easy expansion and replacement.
  - *(8) Testing*
    - Each beamline can be independently taken offline for testing.

Operational and Safety Considerations

- 1.F.2.c Personnel Exclusion Areas
  - *(1) Emergency shut-off devices*
    - Crash buttons are placed in each station.
    - Number and placement is selected to ensure easy access.
  - *(2) Emergency exit mechanisms*
    - All doors are equipped with emergency egress buttons that release the door.
  - *(4) Search procedures*
    - Exclusion area searches are incorporated into the PSS.
- Compliance with APS Facility SAD
  - *DOE requires compliance with the Facility SAD.*

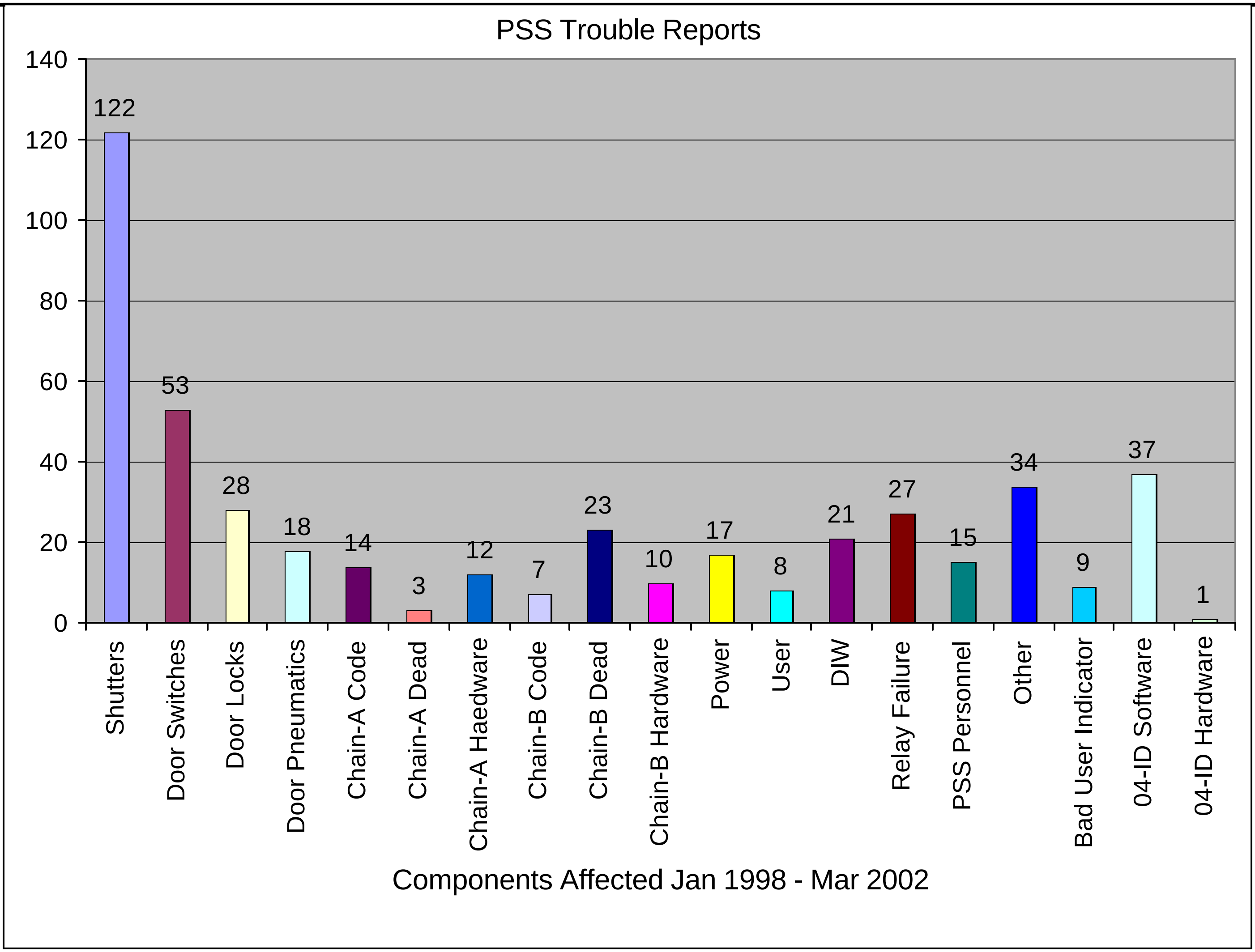
Operational and Safety Considerations

- **Meet the operational and reliability needs of APS machine and beamline operations**
  - Operational Issues
    - *The system will interface to local Touch Screens HMI for control and diagnostics.*
    - *The Touch Screens will have built in help to explain each indicator and control button for each type of screen.*
    - *The system will interface to EPICS for wider dissemination of system status, remote/automated control of experiments and archiving of beamline operations.*

Operational and Safety Considerations

- *Reliability Issues*
  - We have addressed the reliability issues by using reviewed and field tested components from Generation-1 and Generation-2 systems. All of the field devices will be those already approved for use.
  - All hardware will have industrial temperature range specifications.
  - The PSS will be connected to a central UPS.
  - Individual wire terminations have been reduced to field wiring only.
  - Point to point wiring has been eliminated.
  - A review of trouble reports was used to determine and mitigate problem areas.

Operational and Safety Considerations



Operational and Safety Considerations

- *Reliability Issues*
  - While specific fault data has not been analyzed for the period March 2002 to present there is no reason to believe the trend established in this 4 year period for the Generation-1 systems has changed as the Hardware, Software and Configuration remain the same.
  - It should be noted the rightmost 3 columns are specific to the Generation-2 system. The GE Cimplicity software and the Chain-C GE Remote I/O Hardware change out was completed in February 2002. Since the change out the only failure on the beamline with the Generation-2 system was a door lock requiring adjustment. The Bad User Indicator and the 04-ID Software columns present on this chart no longer exist.

System Design Life

- **System should be designed with the intention of building this version for five years and supporting it for ten years**
  - Design Life Goals
    - *Build it for next 5 years minimum.*
    - *Support it for next 10 years minimum.*
    - *Choices for major components are from Allen-Bradley and GE.*
    - *Both vendors inform us they are on a five year cycle with Intel and Motorola for any component containing an embedded microprocessor.*
    - *The affected devices are the PLCs, Touch Screens, networking modules.*
    - *Both vendors assure us availability of either exact or equivalent devices but will not guaranty it in writing.*

System Capabilities

- **Flexibility**
  - The system shall be sufficiently flexible to accommodate all known and anticipated beamline configurations
    - *System flexibility is provided by a modular design.*
    - *You only install what you need.*

- **Expandable**
  - The system shall be sufficiently expandable to accommodate all known and anticipated beamline configurations
    - *The system is expandable by simply adding additional modules where needed.*

System Capabilities

- **Reliability**
  - The system shall be reliable to support the reliability goals of the accelerator and beamlines
    - *The design is based on the field proven design used for Generation-1 and Generation-2 PSS.*

- **Availability**
  - The system shall be easily serviceable to support the availability goals of the accelerator and beamlines
    - *The system is modular minimizing time to repair.*
    - *Repairs can be performed at the module level.*

System Complexity

- **System should not be unnecessarily complicated to operate or support, so as to minimize the possibility of human error during operation, validations, and servicing**
  - System complexity has been kept to a minimum by using a modular design with functional building blocks.
  - Examples of modules are:
    - *De-Ionized Water (DIW) Monitor chassis.*
    - *Front End Shutter Interface Enclosure (FESIE).*
    - *Mezzanine PSS Test Chassis (MPTC).*
  - Additionally point to point wiring has been eliminated and replaced by circuit boards.
  - Factory Molded cables provide all I/O interconnect between the PLCs and the circuit boards.

Standardization

- **System should not be unnecessarily complicated to operate or support, so as to minimize the possibility of human error during operation, validations, and servicing**
  - The system has been designed to accommodate the maximum feasible beamline configuration.
  - The design allows software re-use as standard I/O mapping has been used for all repetitive components such as doors, crash buttons, shutters, search boxes etc.
  - The components used on the floor for field device control will be identical from station to station. The difference will be a count.

Self Diagnostics

- **As much as reasonable, system should provide self-diagnostics for troubleshooting and fault information**
  - The component choices provide diagnostic capability to the point level for shorted outputs.
  - We will use a separate system to cross check the redundant inputs to Chain-A and Chain-B and report differences.
  - Devices that must transition will be checked that they perform as expected – examples are pressure switches, position limit switches, magnetic locks etc.
  - Devices that should be in a certain position at a certain time will be monitored – examples are door closed switches and shutter position limit switches.
  - System communications will be continuously monitored.

Validation Improvement

- **Non-Invasive Validations**
  - Support will be provided for non-invasive PSS validations.
  - Removal and re-connection of existing field wiring should be minimized when performing PSS validations. Connection of additional devices (e.g. to dedicated connectors) is acceptable. Removal of field wiring to make such connections (e.g. as done now for front-end simulator) is not acceptable.
    - *Field device wiring for Chain-A and Chain-B is no longer disconnected to validate.*
    - *The Validation System carts will provide both the means to test the PSS as well as the means to simulate shutters that may not be present.*
    - *We must simulate the Front End Shutters when there is stored beam in the ring.*

Validation Improvement

- **Non-Invasive Validations**
  - Support will be provided for non-invasive PSS validations.
  - Monitoring of PLC status required for PSS validations should not require direct access to the PLC code, as is done now. Hookup of a separate computer is acceptable provided it does not make or facilitate changes in PLC code or checksums.
    - *The Validation System carts will provide the means to test the PSS without being connected to either ESD PLC.*
  - Downloading of PSS code should be streamlined to minimize the possibility of errors
    - *The Validation System carts will provide the means to download the ESD code, Via CDROM.*

Validation Improvement

- **Time Reduction**
  - System design should facilitate reducing PSS validation times
    - *By removing the Command & Control functions to a third system the ESD system the validation times will be reduced.*

- **Validation Quality**
  - There must be no compromise in the system coverage of the validation
    - *The Validation System interface is programmable allowing it to be connected to any beamline configuration.*
    - *The beamline under test is redundantly hardware keyed to identify it for the Validation System as well as for the PSS operational software.*

Validation Improvement

- **Self Test Capabilities**
  - As much as reasonable, system should provide self-test capabilities, e.g. to perform a partial PSS validation with a button push
    - *The Validation System interface is programmable allowing it to be configured to perform these functions.*

EPICS Support

- **All information that could be valuable for operations support shall be provided to EPICS. This included event capture, trending, and problem diagnosis**
  - User Control and Status through EPICS
    - *EPICS will provide all I/O point status along with key internal signal status – examples Beam Ready, APS Enabled etc.*
    - *EPICS can communicate bi-directional with the Command & Control system as it is not part of the safety interlocks.*
    - *The users can request shutter operation through EPICS. It will be granted if all required interlocks are ok.*
    - *Generation-2 users have taken advantage of this interface to automate control of their experiments.*

Backward Compatibility

- **It should be possible to retrofit key benefits of Generation-3 to existing Generation-1 and Generation-2 systems. At a minimum, it should be possible to eliminate needs to remove field wiring when hooking up validation equipment. It is also desirable to provide support for self-test and automated PSS validations, and for other benefits as appropriate.**
  - The path to Retro-fitting Generation-1 & 2 to Generation-3 PSS has been resolved. Since this is a important issue, it will be discussed in detail later in the presentation.

Statement of Work

QUESTIONS?

Day One Complete

Dinner

at

Argonne Guest House